PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-157159
(43)Date of publication of application : 31.05.2002

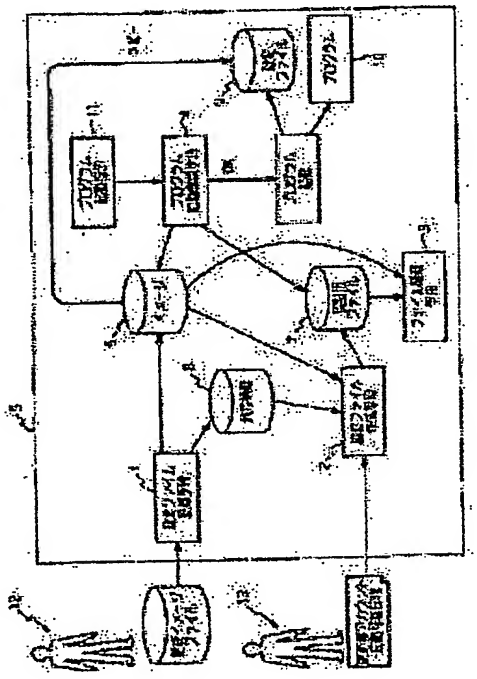
(51)Int.Cl. G06F 12/00
G06F 12/14

(21)Application number : 2000-349719
(22)Date of filing : 16.11.2000

(71)Applicant : NEC CORP
(72)Inventor : KURIMOTO AKANE

(54) UPDATE INFORMATION PROTECTION DEVICE FOR PROGRAM START- UP SETTING FILE

(57)Abstract:
PROBLEM TO BE SOLVED: To provide an update information protection device for a program start-up setting file preventing careless rewriting or falsification of the setting file used at the start-up time of a program to secure safety of the setting file for the program important to system operation.
SOLUTION: In this protection device, by registering the setting file 9 used at the start-up time of the program 10 to a disk as an image 6 and forbidding access to the disk except the start-up time of the program 10, the unjust rewriting to the image 6 that is the setting file 9 for the program start-up is prevented. When starting up the program 10, a program start-up confirmation means 4 decides the presence of the falsification of the image 6, and the program 10 is forbidden to read the image 6 as the setting file 9 when the falsification is present. Thereby, the start-up of the program 10 based on the unjust setting file is prevented.



(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2002－157159
（P2002－157159A）
(43)公開日　平成14年５月31日(2002.5.31)

(51)Int.Cl.'		識別記号	FI		テーマコード'(参考)
Ｇ０６Ｆ	12/00	５３７	Ｇ０６Ｆ 12/00	５３７Ｚ	５Ｂ０１７
	12/14	３１０	12/14	３１０Ｚ	５Ｂ０８２

審査請求　有　請求項の数５　ＯＬ　（全７頁）

(21)出願番号　特願2000－349719(P2000－349719)

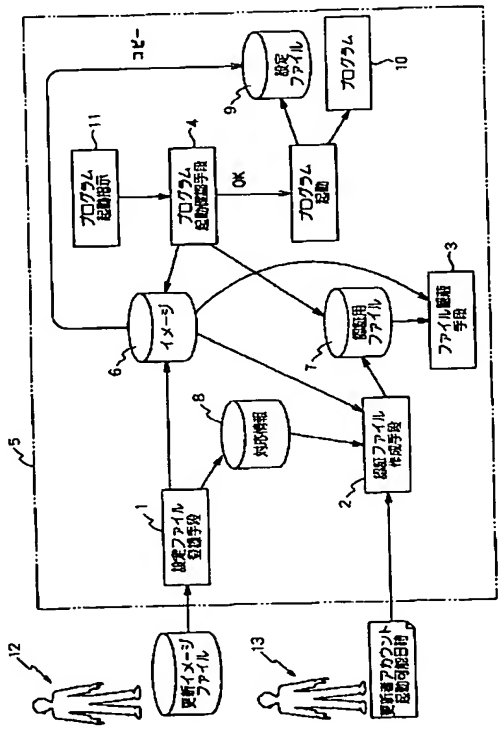
(22)出願日　平成12年11月16日(2000.11.16)

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(72)発明者　栗本　あかね
東京都港区芝五丁目７番１号　日本電気株式会社内
(74)代理人　100079164
弁理士　高橋　勇

Ｆターム(参考)　5B017 AA02 BA06 BB09 CA16
5B082 GA11

(54)【発明の名称】　プログラム起動設定ファイルの更新情報保護装置

(57)【要約】
【課題】　プログラムの起動時に使用される設定ファイルの不用意な書き替えや改竄を防止して、システムの運営上重要なプログラムの設定ファイルの安全を確保することのできるプログラム起動設定ファイルの更新情報保護装置を提供する。
【解決手段】　プログラムの起動時に使用される設定ファイルをイメージ６としてディスクに登録し、プログラムの起動時を除いて当該ディスクへのアクセスを禁止することにより、プログラム起動用の設定ファイル９となるイメージ６に対して不正な書き替えが行われるのを防止する。更に、プログラム起動時にはプログラム起動確認手段４でイメージ６の改竄の有無を判定し、改竄がある場合にはイメージ６を設定ファイル９としてプログラム１０に読み込ませることを禁止することで、不正な設定ファイルに基くプログラム１０の起動を防止する。



1

【特許請求の範囲】

【請求項１】　プログラムの起動時に使用される設定ファイルのイメージをディスクに登録する設定ファイル登録手段と、前記イメージに対する改竄の判定に用いる認証用ファイルを作成して前記ディスクに登録する認証ファイル作成手段と、前記イメージおよび認証用ファイルが格納されているディスクへのアクセスを禁止するファイル隠蔽手段と、前記プログラムに対する起動要求を検出して前記ディスクへのアクセスを許可した後、前記認証用ファイルを用いて前記イメージに対する改竄の有無を判定し、改竄がない場合に限って前記イメージを前記プログラムの起動時に使用される設定ファイルのディレクトリに設定ファイルとして配置し、この設定ファイルに基いて前記プログラムを起動する一方、改竄があった場合には前記ディレクトリへのイメージの配置と前記プログラムの起動を禁止するプログラム起動確認手段とを備えたことを特徴とするプログラム起動設定ファイルの更新情報保護装置。

【請求項２】　前記設定ファイル登録手段は、前記イメージを作成または更新した日時を特定する日時データと前記イメージとの対応関係を記録した対応情報を前記ディスクに登録する機能を有し、前記認証ファイル作成手段は、前記ディスクに登録された対応情報から前記イメージと前記日時データとの対応関係を読み込んで前記認証用ファイルに設定する機能を有し、前記プログラム起動確認手段は、前記ディスクに対応情報として登録された日付データと前記認証用ファイルに設定された日付データとを比較して、両者が一致した場合に限って前記イメージに対する改竄がないものと判定するように構成されていることを特徴とした請求項１記載のプログラム起動設定ファイルの更新情報保護装置。

【請求項３】　前記設定ファイル登録手段は、前記イメージを作成または更新したユーザを特定するユーザアカウントと前記イメージとの対応関係を記録した対応情報を前記ディスクに登録する機能を有し、前記認証ファイル作成手段は、前記イメージとプログラム起動アカウントとの対応関係を前記認証用ファイルに設定する機能を有し、前記プログラム起動確認手段は、前記ディスクに対応情報として登録されたユーザアカウントと前記認証用ファイルに設定されたプログラム起動アカウントとを比較して、両者が一致した場合に限って前記イメージに対する改竄がないものと判定するように構成されていることを特徴とした請求項１または請求項２記載のプログラム起動設定ファイルの更新情報保護装置。

【請求項４】　前記認証ファイル作成手段は、前記イメージを設定ファイルとして利用するプログラムの起動可能日時と前記イメージとの対応関係を前記認証用ファイルに設定する機能を有し、前記プログラム起動確認手段は、前記認証用ファイルに設定された起動可能日時と現在時刻とを比較して、両者が一致した場合に限って前記

2

イメージに対する改竄がないものと判定するように構成されていることを特徴とした請求項１，請求項２または請求項３記載のプログラム起動設定ファイルの更新情報保護装置。

【請求項５】　オペレーティングシステムが備えるアクセス禁止コマンドによって前記ファイル隠蔽手段が構成されていることを特徴とした請求項１，請求項２，請求項３または請求項４記載のプログラム起動設定ファイルの更新情報保護装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、プログラムの起動時に使用される設定ファイルの改竄や不用意な書き替えを防止するプログラム起動設定ファイルの更新情報保護装置に関する。

【０００２】

【従来の技術】プログラムの不正使用を防止するための防衛手段としては、例えば、特開平６－２２３０４０号に開示されるように、プログラムのライセンス数に基いてプログラムの過剰な同時使用を禁止するもの、あるいは、特開平８－３０５５５９号に開示されるように、セーブ日時やプログラム番号および計算機の識別番号に基いてアプリケーションの不正な立ち上げを禁止するものが知られている。

【０００３】

【発明が解決しようとする課題】しかし、これらの従来技術は飽くまでプログラム本体の不正使用を防止するためのものであり、プログラムの使用環境を決める設定ファイルの保護に関しては全く考慮されていない。

【０００４】このため、ファイル転送等によって容易にファイルの書き換えを行うことが可能なＵＮＩＸ（登録商標）等のオープンシステムにおいては、ファイル転送等によって不用意に設定ファイルの内容が書き換えられる可能性があり、システムの運営上重要なプログラム、例えば、ミドルウェアやアプリケーションの設定ファイルの安全が確保されにくいといった問題が生じる場合がある。

【０００５】

【発明の目的】そこで、本発明の目的は、前記従来技術の欠点を解消し、プログラムの起動時に使用される設定ファイルの不用意な書き替えや改竄を防止して、システムの運営上重要なプログラムの設定ファイルの安全を確保することのできるプログラム起動設定ファイルの更新情報保護装置を提供することにある。

【０００６】

【課題を解決するための手段】本発明は、プログラムの起動時に使用される設定ファイルのイメージをディスクに登録する設定ファイル登録手段と、前記イメージに対する改竄の判定に用いる認証用ファイルを作成して前記ディスクに登録する認証ファイル作成手段と、前記イメ

ージおよび認証用ファイルが格納されているディスクへのアクセスを禁止するファイル隠蔽手段と、前記プログラムに対する起動要求を検出して前記ディスクへのアクセスを許可した後、前記認証用ファイルを用いて前記イメージに対する改竄の有無を判定し、改竄がない場合に限って前記イメージを前記プログラムの起動時に使用される設定ファイルのディレクトリに設定ファイルとして配置し、この設定ファイルに基いて前記プログラムを起動する一方、改竄があった場合には前記ディレクトリへのイメージの配置と前記プログラムの起動を禁止するプログラム起動確認手段とを備えたことを特徴とする構成により前記目的を達成した。

【０００７】設定ファイル登録手段は、プログラムの起動時に使用される設定ファイルのイメージをディスクに登録し、また、認証ファイル作成手段は、イメージに対する改竄の判定に用いる認証用ファイルを作成してディスクに登録する。イメージが格納されているディスクへのアクセスはファイル隠蔽手段によって禁止されているので、設定ファイルのイメージの内容がオープンシステムのファイル転送等によって不用意に書き替えられることはなく、また、外部からのアクセスによる不正な書き替えの心配もない。更に、システム管理者や一般ユーザが設定ファイルのイメージや認証用ファイルのディレクトリを特定することも困難であるので、システム管理者や一般ユーザからの不正操作によるイメージや認証用ファイルの改竄も防止される。プログラム起動確認手段は、プログラムに対する起動要求を検出して初めて、イメージと認証用ファイルを格納したディスクへのアクセスを許可し、認証用ファイルを用いて前記イメージに対する改竄の有無を判定する。この段階でイメージに対する改竄が検出された場合には、この設定ファイルのイメージは飽くまでイメージのまま保持され、このイメージが、プログラムの起動時に使用される設定ファイルのディレクトリに移動されることはない。この場合、プログラムの起動も同時に禁止される。従って、仮に、イメージに改竄が施されていたとしても、このイメージが設定ファイルとしてプログラムに読み込まれることはなく、不正な設定ファイルに基くプログラムの起動が未然に防止されることになる。これにより、システムの運営上重要なプログラム、例えば、ミドルウェアやアプリケーション等の誤動作が防止され、安全な処理動作が保証される。また、イメージに対する改竄が検出されなければ、プログラム起動確認手段は、プログラムの起動時に使用される設定ファイルのディレクトリに前記イメージを設定ファイルとして配置し、この段階で初めて、前記イメージが実質的な設定ファイルとして機能することを許容する。この場合、プログラム起動確認手段は、正規のディレクトリに配置された設定ファイルに基いて前記プログラムを起動し、このプログラムを使用した作業の開始を許容する。

【０００８】ここで、設定ファイル登録手段には、イメージを作成または更新した日時を特定する日時データとイメージとの対応関係を記録した対応情報をディスクに登録する機能を持たせ、また、認証ファイル作成手段には、ディスクに登録された対応情報からイメージと日時データとの対応関係を読み込んで認証用ファイルに設定する機能を持たせることができる。対応情報はイメージと一体化しても構わない。この場合、プログラム起動確認手段は、ディスクに対応情報として登録された日付データと認証用ファイルに設定された日付データとを比較して、両者が一致した場合に限ってイメージに対する改竄がないものと判定するように構成する。

【０００９】このような構成によれば、認証ファイル作成後の不正操作によって改竄されたイメージが設定ファイルとして機能したり、不正なイメージを設定ファイルとして使用したプログラムの起動を未然に防止することができる。

【００１０】また、イメージを作成または更新したユーザを特定するユーザアカウントとイメージとの対応関係を記録した対応情報をディスクに登録する機能を設定ファイル登録手段に持たせ、認証ファイル作成手段には、イメージとプログラム起動アカウントとの対応関係を認証用ファイルに設定する機能を持たせることができる。対応情報はイメージと一体化しても構わない。この場合、プログラム起動確認手段は、ディスクに対応情報として登録されたユーザアカウントと認証用ファイルに設定されたプログラム起動アカウントとを比較し、両者が一致した場合に限ってイメージに対する改竄がないものと判定するように構成する。

【００１１】これにより、プログラムを起動する使用権のないユーザが作成または更新したイメージが設定ファイルとして機能したり、不正なイメージを設定ファイルとして使用したプログラムの起動を未然に防止することができる。

【００１２】更に、プログラムの起動可能日時とイメージとの対応関係を認証用ファイルに設定する機能を認証ファイル作成手段に持たせ、認証用ファイルに設定された起動可能日時と現在時刻とを比較して、両者が一致した場合に限ってイメージに対する改竄がないものと判定するようにプログラム起動確認手段を構成することも可能である。

【００１３】このような構成によれば、予め設定された日時以外にプログラムが不正に起動されるのを防止することができる。

【００１４】また、ファイル隠蔽手段は、オペレーティングシステムが備えるアクセス禁止コマンドを利用して構成することができる。

【００１５】オペレーティングシステムが備えるアクセス禁止コマンドを利用することにより、設定ファイルのイメージおよび認証用ファイルを容易に隠蔽することが

可能となる。

【００１６】

【発明の実施の形態】以下、図面を参照して本発明の一実施形態について詳細に説明する。図１は本発明を適用した一実施形態のプログラム起動設定ファイルの更新情報保護装置の構成の概略を示した機能ブロック図である。

【００１７】このうち、更新情報保護装置の主要部を形成する設定ファイル登録手段１と認証ファイル作成手段２およびファイル隠蔽手段３とプログラム起動確認手段４の各々は、実質的に、オープンシステム５内、例えば、UNIXマシン内に設置されたプログラムによって構成される。

【００１８】設定ファイル登録手段１で作成された設定ファイルのイメージ６と対応情報８、および、認証ファイル作成手段２で作成された認証用ファイル７は、オープンシステム５内のディスク、つまり、ハードディスク等の記憶装置に格納される。

【００１９】また、ファイル隠蔽手段３は、オープンシステム５のオペレーティングシステムが標準的に備えるアクセス禁止コマンド、例えば、HP-UXにおけるvgreduceコマンド等を使用して、イメージ６，認証用ファイル７，対応情報８を格納したディスクへの外部および内部からのアクセスを禁止するようになっている。

【００２０】設定ファイル登録手段１は、プログラムの起動時に使用される設定ファイルの作成あるいは更新の際に使用されるが、ここで作成された設定ファイルは、プログラムの起動時に設定ファイルの読み込みに使用されるディレクトリ、つまり、図１に示されるような設定ファイル９の位置には直ちに配置されず、前述したアクセス禁止の設定が可能なディスク内にそのまま保持される。

【００２１】この実施形態では、プログラムの起動時に設定ファイルの読み込みに使用されるディレクトリに置かれた設定ファイル、要するに、実際にプログラムの立ち上げに使用される設定ファイルを設定ファイル９と呼び、また、アクセス禁止の設定が可能なディスク内に保持された設定ファイルのことを単にイメージ６と呼んでいる。設定ファイル登録手段１で作成された設定ファイルのイメージ６が適切なものである限り、実質的に、イメージ６と設定ファイル９の内容は同一である。

【００２２】ここでいう設定ファイルとは、例えば、プログラムの実行に必要とされるパラメータを保存したファイル、あるいは、複数の一般ユーザが同一プログラムを使用する際に使用する各ユーザ毎の環境設定ファイル等である。

【００２３】プログラム起動確認手段４には、ミドルウェアやアプリケーション等のプログラム１０を起動するためのイベントであるプログラム起動指示１１を検出してディスクに対するアクセス禁止設定を解除し、イメージ６，認証用ファイル７，対応情報８にアクセスする機能があり、このプログラム起動指示１１を検出した段階で、プログラム起動確認手段４が前述した認証用ファイル７を使用してイメージ６に対する改竄の有無を判定する。

【００２４】そして、改竄がないと判定された場合に限り、プログラム起動確認手段４は、イメージ６を設定ファイルの正規のディレクトリ、つまり、図１に示される９の位置にコピーして、このコピー（イメージ）を正規の設定ファイル９とし、この設定ファイル９の内容に基いてプログラム１０を起動する。

【００２５】また、改竄があると判定された場合には、プログラム起動確認手段４は、正規のディレクトリへのイメージ６のコピーを非実行とし、プログラム１０の起動も禁止する。

【００２６】以下、図１の機能ブロック図と各手段の処理動作の概略を示した図２～図４のフローチャートを参照して、本実施形態の更新情報保護装置の処理動作について詳細に説明する。

【００２７】図２は設定ファイル登録手段によって実行される設定ファイル登録処理について示したフローチャートである。

【００２８】まず、一般ユーザ１２がパラメータや環境設定関係等の設定ファイルを作成あるいは更新し、この設定ファイルをユーザアカウント（ユーザを識別するためのコード）と共に設定ファイル登録手段１に入力する（ステップａ１）。設定ファイルの作成あるいは更新を行う一般ユーザは単数であっても複数であっても構わない。

【００２９】設定ファイル登録手段１は、入力された設定ファイルをイメージ６としてディスクに格納し（ステップａ２）、更に、今回作成されたイメージ６とこれを作成したユーザおよび現在時刻との対応関係を記憶した対応情報８を作成してディスクに格納する（ステップａ３）。この場合のユーザとは具体的にはユーザアカウントの値である。また、ユーザアカウントおよび現在時刻はイメージ６自体にも添付される。

【００３０】次に、認証ファイル作成手段２を利用したシステム管理者側の作業が行われることになる。

【００３１】図３は認証ファイル作成手段２によって実行される認証用ファイル作成処理について示したフローチャートである。

【００３２】システム管理者１３は、まず、認証ファイル作成手段２を用いて、プログラムの起動可能日時とユーザアカウント（この場合は一般ユーザ１２のユーザアカウント）等を入力する（ステップｂ１）。

【００３３】すると、この入力操作を検出した認証ファイル作成手段２は、システム管理者１３が入力したユーザアカウントに基いてディスク内の対応情報を検索し、該当する一般ユーザ１２の対応情報８を抽出して、イメ

ージ６の情報と該イメージ６の作成日時（イメージ作成時に記録された現在時刻）を取得し（ステップｂ２）、モニタ画面に一般ユーザ１２が作成したイメージ６の内容、つまり、一般ユーザ１２が作成あるいは更新した設定ファイルの内容を表示する（ステップｂ３）。

【００３４】次いで、システム管理者１３は、モニタ画面に表示された設定ファイルの内容を確認し、問題がなければ、このイメージ６を設定ファイル９として使用することを許諾し、認証ファイル作成手段２による認証用ファイル７の作成を実行させる（ステップｂ４）。この認証用ファイル７には、イメージ６の作成日時と、このイメージ６を作成あるいは更新した一般ユーザ１２のユーザアカウント（プログラム起動アカウント）、および、前述したステップｂ１の処理でシステム管理者１３が設定したプログラムの起動可能日時が記録される。

【００３５】そして、認証ファイル作成手段２はファイル隠蔽手段３を作動させ、設定ファイル登録手段１によって作成されたイメージ６と認証ファイル作成手段２によって作成された認証用ファイル７の格納されているディスクをオペレーティングシステムの機能、例えば、HP-UXにおけるvgreduceコマンド等を使用してアクセスできない状態にする（ステップｂ５）。

【００３６】次に、図４に示す起動確認処理のフローチャートを参照してプログラム起動確認手段４の処理動作について説明する。

【００３７】プログラム１０を起動するためのイベントであるプログラム起動指示１１がプログラム起動確認手段４によって検出されると、プログラム起動確認手段４は、まず、ファイル隠蔽手段３によるアクセス禁止設定をオペレーティングシステムの機能、例えば、HP-UXにおけるvgextendコマンド等を使用して解除し（ステップｃ１）、当該プログラム１０の起動に必要とされる設定ファイル９に対応するイメージ６を参照して（ステップｃ２）、このイメージ６に添付された作成日付と認証用ファイル７に記録されたイメージ６の作成日付とが一致しているか否かを判定する（ステップｃ３）。

【００３８】更に、両者が一致している場合には、当該プログラム１０の起動に必要とされる設定ファイル９に対応するイメージ６の認証用ファイル７を参照して（ステップｃ４）、認証用ファイル７に記録された起動可能日時と現在時刻、および、認証用ファイル７に記録されたプログラム起動アカウントとイメージ６に添付されたユーザアカウントとを比較する（ステップｃ５）。

【００３９】そして、作成日付，起動可能日時，ユーザアカウントの全てが一致した場合にはイメージ６に不適当な改竄がないものと判定し、プログラム起動確認手段４は、図１に示されるようにして、プログラム１０の起動に必要とされる設定ファイル９に対応するイメージ６を正規のディレクトリにコピーして設定ファイル９を生成し（ステップｃ６）、この設定ファイル９の設定、例えば、パラメータや環境設定等を利用してプログラム１０を起動した後、再びファイル隠蔽手段３を使用して、ディスクに対するアクセスを禁止の状態とする。

【００４０】一方、ステップｃ３あるいはステップｃ５の判定処理において、作成日付，起動可能日時，ユーザアカウントの何れかに不一致が認められた場合には、プログラム起動確認手段４は、イメージ６に不適切な改竄があるものと判定し、ステップｃ６におけるイメージのコピー処理を非実行として、プログラム１０の起動も禁止する（ステップｃ７）。

【００４１】以上に述べた通り、設定ファイルのイメージ６が格納されているディスクへのアクセスは、プログラム１０の起動時を除き、ファイル隠蔽手段３によって常に禁止の状態とされているので、一旦設定されたイメージ６の内容がファイル転送等によって不用意に書き替えられることはなく、また、外部からのアクセスによる不正な書き替えの心配もない。更に、システム管理者１３や一般ユーザ１２がイメージ６や認証用ファイル７のディレクトリを特定することも事実上不可能であるので、システム管理者１３や一般ユーザ１２からの不正操作によるイメージ６や認証用ファイル７の改竄も未然に防止される。

【００４２】プログラム起動確認手段４は、プログラム１０に対するプログラム起動指示１１を検出して初めて、イメージ６と認証用ファイル７を格納したディスクへのアクセスを許可し、イメージ６に不適当な改竄がない場合に限ってイメージ６をプログラム起動用の正規のディレクトリにコピーして設定ファイル９としての使用を許可する一方、イメージ６に不適当な改竄が認められた場合には、イメージ６のコピー処理、つまり、イメージ６を設定ファイル９として使用することを禁止するようにしているので、仮に、イメージ６に改竄が施されていたとしても、このイメージ６が設定ファイル９としてプログラム１０に読み込まれることはなく、不正な設定ファイルに基くプログラム１０の起動が未然に防止される。よって、システムの運営上重要なプログラム、例えば、ミドルウェアやアプリケーション等の安全が処理動作が確保される。

【００４３】また、イメージ６の改竄の判定に用いるデータとしては、イメージ６の作成日付およびプログラム１０の起動可能日時とプログラム起動アカウントとを並列的に利用するようにしているので、認証ファイル７を作成した後の不正操作によるイメージ６の改竄や、規定時間外のプログラム１０の不正な立ち上げ、更には、プログラム１０を起動する使用権のないユーザ１２によるプログラム１０の不正使用も未然に防止することができる。

【００４４】イメージ６の改竄の判定に用いるデータとしては、前述した作成日付，起動可能日時，プログラム起動アカウントの他にも、イメージ６のファイルサイズ

や有効時間等を利用することが可能である。

【００４５】イメージ６のファイルサイズを判定データとして利用する場合には、イメージ６の作成時にそのファイルサイズを測定してイメージ６に添付すると共に、このファイルサイズを認証用ファイル７にも記録する。そして、プログラム起動指示１１が検出された時点で、イメージ６のファイルサイズを再び測定して認証用ファイル７に記録されているファイルサイズと比較し、ファイルサイズの一致不一致によってイメージ６の改竄の有無を判定するようにする。

【００４６】有効時間を判定データとして利用する場合の処理に関しては、前述した起動可能日時の場合と同様である。

【００４７】また、イメージ６の作成時にイメージ６自体のコピーを保存しておき、プログラム１０の起動時にイメージ６とそのコピーとを直接比較したり、あるいは、差分の有無を測定することによって改竄の有無を判定するようにしてもよい。

【００４８】

【発明の効果】本発明によるプログラム起動設定ファイルの更新情報保護装置は、プログラムの起動時に使用される設定ファイルをイメージとしてディスクに登録し、プログラムの起動時を除いて当該ディスクへのアクセスを禁止するようにしているので、設定ファイルのイメージの内容がオープンシステムのファイル転送等によって不用意に書き替えられることはなく、また、外部からのアクセスによる不正な書き替えも未然に防止することができる。また、ディスクへのアクセスが禁止される結果、システム管理者や一般ユーザが設定ファイルのイメージのあるディレクトリを特定することも事実上不可能であり、システム管理者や一般ユーザからの不正操作によるイメージの改竄や上書きも防止される。更に、プログラム起動確認手段は、プログラムに対する起動要求を検出して初めて、イメージを格納したディスクへのアクセスを許可し、認証用ファイルを用いてイメージに対する改竄の有無を判定すると共に、イメージに改竄がない場合に限ってイメージを正規のディレクトリに配置してプログラム起動用の設定ファイルとする一方、イメージに改竄が検出された場合には、このイメージを設定ファイルのディレクトリに移動することを禁止し、同時に、プログラムの起動も禁止するようにしているので、仮に、イメージに改竄が施されていたとしても、このイメージが設定ファイルとしてプログラムに読み込まれることはなく、不正な設定ファイルに基くプログラムの起動を未然に防止することができる。従って、システムの運営上重要なプログラム、例えば、ミドルウェアやアプリケーション等の安全な処理動作を確保することができる。

【００４９】特に、イメージを作成または更新した日時を特定する日時データや、イメージを作成または更新したユーザを特定するユーザアカウント、更には、プログラムの使用を許可する起動可能日時を改竄判定のデータとして適用することにより、認証ファイル作成後の不正操作によって改竄されたイメージの不正使用や、プログラムを起動する使用権のないユーザによるプログラムの不正使用、および、時間外のプログラムの不正使用を確実に防止することができる。

【００５０】更に、ファイル隠蔽手段は、オペレーティングシステムが備えるアクセス禁止コマンドを利用してディスクを隠蔽するようにしているので、複雑なプログラムを作成することなく、設定ファイルのイメージや認証用ファイルを確実に隠蔽することができる。

【図面の簡単な説明】

【図１】本発明を適用した一実施形態のプログラム起動設定ファイルの更新情報保護装置の構成の概略を示した機能ブロック図である。

【図２】設定ファイル登録手段によって実行される設定ファイル登録処理について示したフローチャートである。

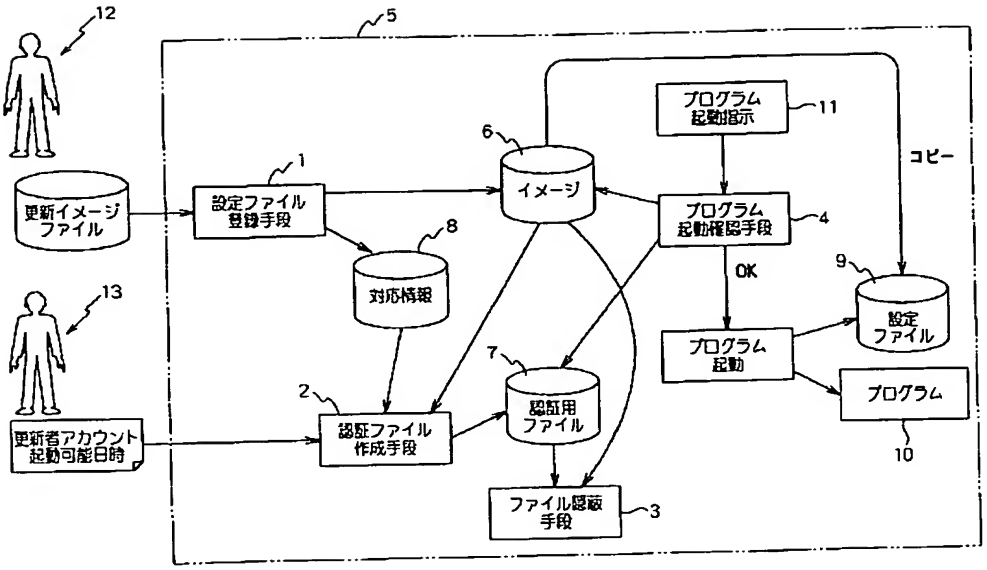
【図３】認証ファイル作成手段によって実行される認証用ファイル作成処理について示したフローチャートである。

【図４】プログラム起動確認手段によって実行される起動確認処理について示したフローチャートである。

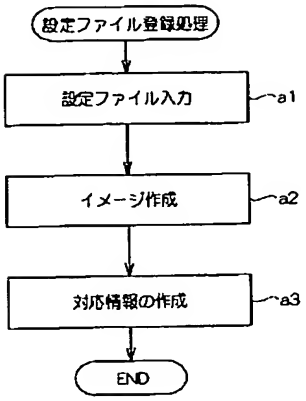
【符号の説明】

１　設定ファイル登録手段
２　認証ファイル作成手段
３　ファイル隠蔽手段
４　プログラム起動確認手段
５　オープンシステム
６　設定ファイルのイメージ
７　認証用ファイル
８　対応情報
９　設定ファイル
１０　プログラム
１１　プログラム起動指示
１２　一般ユーザ
１３　システム管理者

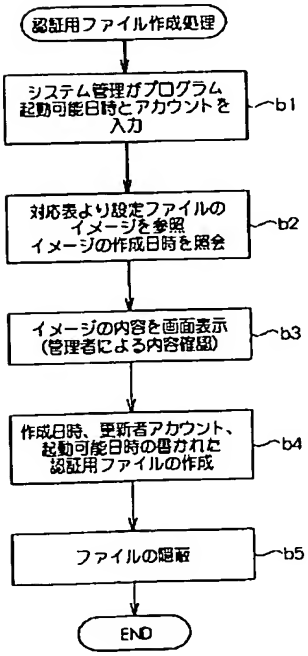
【図１】


12
5
更新イメージファイル
設定ファイル登録手段
1
イメージ
6
プログラム起動指示
11
コピー
プログラム起動確認手段
4
8
対応情報
OK
9
設定ファイル
13
7
2
認証用ファイル
プログラム起動
プログラム
10
更新者アカウント起動可能日時
認証ファイル作成手段
ファイル隠蔽手段
3

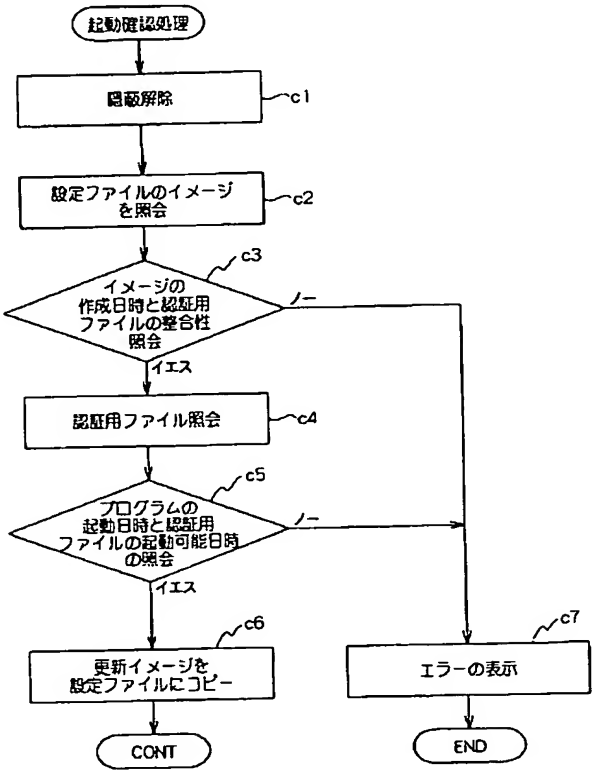
【図２】


設定ファイル登録処理
設定ファイル入力
a1
イメージ作成
a2
対応情報の作成
a3
END

【図３】


認証用ファイル作成処理
システム管理がプログラム起動可能日時とアカウントを入力
b1
対応表より設定ファイルのイメージを参照イメージの作成日時を照会
b2
イメージの内容を画面表示(管理者による内容確認)
b3
作成日時、更新者アカウント、起動可能日時の書かれた認証用ファイルの作成
b4
ファイルの隠蔽
b5
END

【図４】


起動確認処理
隠蔽解除
c1
設定ファイルのイメージを照会
c2
c3
イメージの作成日時と認証用ファイルの整合性照会
ノー
イエス
認証用ファイル照会
c4
c5
プログラムの起動日時と認証用ファイルの起動可能日時の照会
ノー
イエス
c6
更新イメージを設定ファイルにコピー
CONT
c7
エラーの表示
END